REMARKS

The Examiner is thanked for the performance of a thorough search.

In the specification, paragraph [0001] has been amended to indicate the now-abandoned status of U.S. Patent Application No. 09/393,410.

By this amendment, Claims 8, 10, 12, 16, 18, 27, and 29 have been amended. No claims have been added or canceled. Hence, Claims 1-30 are pending in the application.

SUMMARY OF THE REJECTIONS

Claims 8, 10, 12-19, 27, and 29 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite.

Claims 1, 3, 11, 12, 19, 22, 22, and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 4,200,770 to Hellman et al. ("Hellman") in view of U.S. Patent No. 5,841,864 to Klayman et al. ("Klayman").

Claims 2, 4-7, 13-15, 21, and 23-26 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hellman in view of Klayman and U.S. Patent No. 5,633,933 to Aziz ("Aziz").

Claims 8, 10, 16, 18, 27, and 29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hellman in view of Klayman and *Handbook of Applied Cryptography* by Alfred J. Menezes et al. ("Menezes").

Claims 9, 17, and 28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hellman in view of Klayman and U.S. Patent No. 6,363,154 to Peyravian et al. ("Peyravian").

THE REJECTIONS NOT BASED ON THE PRIOR ART

Rejections Based on 35 U.S.C. § 112, Second Paragraph

Claims 8, 10, 12-19, 27, and 29 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Those of the claims that contained the word "approximately" have been amended so that they no longer contain the word "approximately." Claim 12 has been amended to define "n." Those of the claims that contained the word "whereby" have been amended so that they no longer contain the word "whereby." Therefore, the withdrawal of all of the rejections under 35 U.S.C. § 112, second paragraph, is respectfully requested.

THE REJECTIONS BASED ON THE PRIOR ART

Rejections Based on 35 U.S.C. § 103(a)

Claims 1, 3, 11, 12, 19, 20, 22, and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hellman in view of Klayman. Claims 2, 4-7, 13-15, 21, and 23-26 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hellman in view of Klayman and Aziz. Claims 8, 10, 16, 18, 27, and 29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hellman in view of Klayman and Menezes. Claims 9, 17, and 28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hellman in view of Klayman and Peyravian. The rejections of Claims 1-30 are traversed.

Claims 1, 3, 11, 20, 22, and 30

Claim 1 requires, among other features, "receiving from the second node a second private value associated with the second node using the intermediate shared key." The Office Action alleges that Hellman discloses receiving a value from a node, but concedes that Hellman fails to

teach or suggest that such a value is private. The Office Action does not even allege that Klayman teaches or suggests that such a value is private. Instead, the Office Action asserts that it would have been obvious to transmit a private value because (1) very few have access to private values, (2) private values are more difficult to decipher, and (3) using a combination of two private values creates a more secure public cipher.

However, it does not necessarily follow, merely from the fact that very few have access to a private value, that the private value should be transmitted. Traditionally, private values have not been transmitted or shared because doing so almost certainly would compromise the security of the cryptosystem. Indeed, the non-shared nature of private values is precisely what makes those values private. The fact that a private value is not widely possessed is not a valid reason for transmitting that private value.

Additionally, private values are not necessarily more difficult to decipher than public values. Indeed, private values traditionally have not been encrypted; traditionally, there has been no need to encrypt private values because they have been, not surprisingly, kept private. Because private values traditionally have not been encrypted in the first place, it cannot be said that private values have been or are "more difficult to decipher." The act of deciphering traditionally is not an act that has been applicable to unencrypted values.

The Office Action asserts that using a combination of two private values to generate a public cipher makes that public cipher more secure. Although this is an interesting hypothesis, it is only that. The Office Action adduces no evidence whatsoever in support of this hypothesis. The Office Action does not explain why a public cipher that was generated using a combination of two private values would be more secure than, say, a public cipher that was generated using only one private value having a length in bits far longer than the two values. None of the

references cited by the Office Action appear to lend any credence to this theory. It is respectfully submitted that the notion that "using a combination of two private values to generate a public cipher makes that public cipher more secure" is not well known or recognized, even today. The mere declaration in an Office Action that a proposition is true, without some kind of rationale or support, does not properly support a §103 rejection.

Even if the use of a combination of two private values to generate a public cipher made that public cipher more secure, this would not necessarily be a reason for either of the two private values to be transmitted between nodes. If the notion were true, then a single node could use a combination of two private values to generate a public cipher without ever sending or receiving either of the private values; the node could generate both of the private values.

Claim 1 also requires, among other features, "communicating a collective public key that is based upon the first private value and the second private value to a third node of the network," "receiving an individual public key from the third node," and "computing and storing the group shared secret key based upon the individual public key." The Office Action concedes that Hellman does not disclose any of these features. The Office Action does not even allege that Klayman teaches or suggests any of these features. Instead, the Office Action characterizes all of these features as a repetition of the Diffie-Hellman exchange, only using different public keys than those that were used in the earlier iteration, and then contends that a mere duplication of a procedure is obvious because such a duplication requires only routine skill in the art. The Office Action relies on *In re Harza,* 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960) to support this contention.

However, the Office Action has taken *In re Harza* out of context. Although *Harza* held that the mere duplication of **mechanical parts** has no patentable significance unless the

duplication produces a new and unexpected result, *Harza* did **not** hold that the duplication of **procedures** has no patentable significance.

Besides this, though, the "procedures" recited in Claim 1 are not "mere duplications." Claim 1 recites that the "collective public key" is based upon a first private value and a second private value, where the second private value was received from a second node using an intermediate shared key. The Diffie-Hellman exchange does not involve the generation of a collective public key using a private value received from another node. Instead, in the Diffie-Hellman exchange, private keys (the "first signal" and "second signal" referred to in Hellman, col. 2, lines 35-53) are kept secret by their respective "conversers" and are not sent to other "conversers." Only the public keys (the "transformed first signal" and "transformed second signal" referred to in Hellman, col. 2, lines 35-53) are transmitted between the "conversers." Because the Diffie-Hellman exchange does not involve an exchange having the qualities of the "procedures" recited in Claim 1—namely, the receipt of a private value that is associated with another node—the "procedures" recited in Claim 1 are not "mere duplications" of procedures involved in the Diffie-Hellman exchange.

In *Harza*, the disputed claim, which recited a plurality of ribs, was unpatentable over the prior art, which recited only the equivalent of one rib, because the addition of ribs did not cause any different result from that achieved by the prior art. However, in the present application, the "procedures" claimed allow a group secret shared key for N nodes to be computed using less than N * (N-1) messages. This is a new and unexpected result. Unlike *Harza's* ribs, each of which performed the same function no matter how many other ribs it joined, the "procedures" recited in Claim 1 produce different results than any that came before. For example, using the method of Claim 1, the recited "group shared secret key" can be used to communicate data

securely between three nodes, but the "intermediate shared secret key" recited in Claim 1 only can be used to communicate data securely between two nodes. Each successively generated secret key performs a different function than the secret key that was generated before it. The values used to generate each successive secret key also differ from the values used to generate previous secret keys. Each successive generation of a secret key builds upon the generation before, which saves time and effort.

"Merely duplicating" the Diffie-Hellman exchange was precisely what was done prior to the method recited in Claim 1. Such a "mere duplication" approach is described in the Background section of the present application (see pages 6 and 7). Because each exchange was a point-to-point exchange that involved only two nodes, the "mere duplication" approach required no less than N * (N-1) messages to distribute, among N nodes, information that could be used to arrive at a group shared secret key. In contrast, the method of Claim 1 allows a group shared secret key to be computed using less than N * (N-1) messages. By the way, this difference is expressly recited in Claim 1.

Two different processes, sufficiently abstracted, can always be made to seem alike. One might try to say that a dog, having a head and four limbs, is not significantly different from a man who also possesses those traits. However, it is not proper to abstract the limitations of a claim to the extent that the more detailed and distinguishing aspects of those limitations are ignored through the abstraction, and then to say, because of the ignorance, that the limitations are no different than what was already known. The details make the difference. If such unbounded abstraction were permissible in evaluating the patentability of a claim, then no claim would ever be allowable. Although Diffie-Hellman and the method of Claim 1 both involve the exchange of public keys to one extent or another, the differences between the two are significant.

For at least the reasons discussed above, it is respectfully submitted that Claim 1 is patentable over Hellman and Klayman.

Claims 3 and 11 depend from Claim 1 and therefore include the features of Claim 1 that are distinguished from Hellman and Klayman above. Therefore, for at least the reasons discussed above with relation to Claim 1, it is respectfully submitted that Claims 3 and 11 are patentable over Hellman and Klayman.

Claim 20, 22, and 30 recite computer-readable media carrying instructions that, when executed, cause one or more processors to perform the steps of the methods of Claims 1, 3, and 11, respectively. Therefore, for at least the reasons discussed above with regard to Claims 1, 3, and 11, it is respectfully submitted that Claims 20, 22, and 30 are patentable over Hellman and Klayman.

Claims 12 and 19

The Office Action appears to reject Claim 12 on the same bases as Claim 1, even though the limitations of Claim 12 and Claim 1 are different. Claim 12 requires, among other features, "computing a second shared secret key based upon the second public key, the first message, and the second message." The Office Action does not even allege, specifically, that either Hellman or Klayman teaches or suggests this feature of Claim 12.

The Office Action does allege that "computing and storing the group shared secret key based upon the individual public key," as recited in Claim 1, is a "mere duplication" of the Diffie-Hellman exchange. To the extent that the Office Action meant to reject the above-quoted feature of Claim 12 based on the rationale extended for rejecting the above-quoted feature of Claim 1, it is respectfully submitted that Hellman and Klayman do not teach and suggest the

above-quoted feature of Claim 12 for at least the same reasons, discussed above in relation to Claim 1, that Hellman and Klayman fail to teach or suggest the above-quoted feature of Claim 1.

For at least the reasons discussed above, it is respectfully submitted that Claim 12 is patentable over Hellman and Klayman.

Claim 19 depends from Claim 12 and therefore includes the features of Claim 12 that are distinguished from Hellman and Klayman above. Therefore, for at least the reasons discussed above with relation to Claim 12, it is respectfully submitted that Claim 19 is patentable over Hellman and Klayman.

Claims 2, 4-7, 21, and 23-26

Claims 2 and 4-7 depend from Claim 1 and therefore include the features of Claim 1 that are distinguished from Hellman and Klayman above. Aziz also fails to teach or suggest these features. Indeed, the Office Action does not even allege that Aziz teaches or suggests these features. Therefore, it is respectfully submitted that Claims 2 and 4-7 are patentable over Hellman, Klayman, and Aziz.

Claims 21 and 23-26 recite computer-readable media carrying instructions that, when executed, cause one or more processors to perform the steps of the methods of Claims 2 and 4-7, respectively. Therefore, for at least the reasons discussed above with regard to Claims 2 and 4-7, it is respectfully submitted that Claims 21 and 23-26 are patentable over Hellman, Klayman, and Aziz.

Claims 13-15

Claims 13-15 depend from Claim 12 and therefore include the features of Claim 12 that are distinguished from Hellman and Klayman above. Aziz also fails to teach or suggest these features. Indeed, the Office Action does not even allege that Aziz teaches or suggests these features. Therefore, it is respectfully submitted that Claims 13-15 are patentable over Hellman, Klayman, and Aziz.

Claims 8, 10, 27, and 29

Claims 8 and 10 depend from Claim 1 and therefore include the features of Claim 1 that are distinguished from Hellman and Klayman above. Menezes also fails to teach or suggest these features. Indeed, the Office Action does not even allege that Menezes teaches or suggests these features. Therefore, it is respectfully submitted that Claims 8 and 10 are patentable over Hellman, Klayman, and Menezes.

Claims 27 and 29 recite computer-readable media carrying instructions that, when executed, cause one or more processors to perform the steps of the methods of Claims 8 and 10, respectively. Therefore, for at least the reasons discussed above with regard to Claims 8 and 10, it is respectfully submitted that Claims 27 and 29 are patentable over Hellman, Klayman, and Menezes.

Claims 16 and 18

Claims 16 and 18 depend from Claim 12 and therefore include the features of Claim 12 that are distinguished from Hellman and Klayman above. Menezes also fails to teach or suggest these features. Indeed, the Office Action does not even allege that Menezes teaches or suggests

these features. Therefore, it is respectfully submitted that Claims 16 and 18 are patentable over Hellman, Klayman, and Menezes.

Claims 9 and 28

Claim 9 depends from Claim 1 and therefore includes the features of Claim 1 that are distinguished from Hellman and Klayman above. Peyravian also fails to teach or suggest these features. Indeed, the Office Action does not even allege that Peyravian teaches or suggests these features. Therefore, it is respectfully submitted that Claim 9 is patentable over Hellman, Klayman, and Peyravian.

Claim 28 recites a computer-readable medium carrying instructions that, when executed, cause one or more processors to perform the steps of the method of Claim 9. Therefore, for at least the reasons discussed above with regard to Claim 9, it is respectfully submitted that Claim 28 is patentable over Hellman, Klayman, and Peyravian.

Claim 17

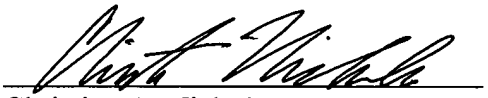
Claim 17 depends from Claim 12 and therefore includes the features of Claim 12 that are distinguished from Hellman and Klayman above. Peyravian also fails to teach or suggest these features. Indeed, the Office Action does not even allege that Peyravian teaches or suggests these features. Therefore, it is respectfully submitted that Claim 17 is patentable over Hellman, Klayman, and Peyravian.

CONCLUSION

It is respectfully submitted that all of the pending claims are in condition for allowance and the issuance of a notice of allowance is respectfully requested. If there are any additional charges, please charge them to Deposit Account No. 50-1302.

The Examiner is invited to contact the undersigned by telephone if the Examiner believes that such contact would be helpful in furthering the prosecution of this application.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP



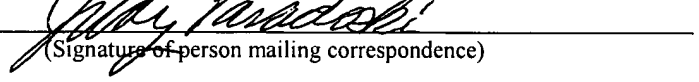
Dated: December 21, 2004

Christian A. Nicholes
Reg. No. 50,266

Christian A. Nicholes
2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
(408) 414-1080
Facsimile: (408) 414-1076

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on
December 21, 2004
(Date of Deposit)

Judy Paradoski
(Typed or printed name of person mailing correspondence)



(Signature of person mailing correspondence)